Inspection and Incident Reporting Instructions:
At each merchant's discretion, develop a schedule or routine to inspect devices to look for tampering or substitution periodically.

For Clover P2PE Device, please refer to page 57 to Page 69 in the Clover P2PE Implementation Manual for inspection instruction, tamper monitoring, skimming prevention and encryption issue handling.

The Clover P2PE Implementation Manual is available upon request. Please contact pci-compliance@stanford.edu if you would like to get a soft copy of Clover P2PE Implementation Manual.

If any suspicion is detected during the inspection, please follow page 63 - 64 for contacting Clover or email support@clover.com or call 855-853-8340. You can also contact pci-security@stanford.edu.

For other devices, please contact the device distributors for detailed instructions. The rule of thumb is to check any overlays, wires, cutting, disassembly, addition, modification, scratches or tampering, no changes to the resistance when inserting or removing a card from the ICC slot.
If any suspicion is detected during the inspection, please follow the manufacturer’s manual instruction for reporting or contact pci-security@stanford.edu.

PCI DSS Compliance Annual Validation:
Each merchant department using Clover P2PE device should fill out, at least, SAQ P2PE-HW form annually.

When FD400 or other dial-up POS devices are used, the merchant department should fill out, at least, SAQ B form annually.

For the merchant departments using multiple types of devices and other payment processing methods, please contact pci-compliance@stanford.edu for further consultation.

Other relevant references available in https://pcicompliance.stanford.edu:
Please refer to the PCI DSS 3.2.1 for 9.9.2 and 9.9.3 details.
Please refer to Skimming Prevention: Best Practices for Merchants.
Please refer to Stanford PCI Policy 24 Media Device Protection Policy

For any further questions, please contact pci-compliance@stanford.edu.